CLAIMS

1. A computer-implemented method for restricting use of a clipboard application in a multi-application computing environment, said method comprising:

receiving a copy selection associated with designated content of a source file being displayed by a source application;

determining whether the source file is a secured file; and

preventing subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file.

2. A computer-implemented method as recited in claim 1, wherein said method further comprises:

receiving a paste selection to provide the designated content to the destination application.

3. A computer-implemented method as recited in claim 2, wherein the paste selection requests to paste the designated content to a destination file that is opened within the destination application.

4. A computer-implemented method as recited in claim 2, wherein the copy selection is a copy command, and wherein the paste selection is a paste command.

5. A computer-implemented method as recited in claim 1, wherein said determining operates to determine that the source file is a secured file based on security information provided by the source application.

6. A computer-implemented method as recited in claim 5, wherein the security information pertains to the source document.

7. A computer-implemented method as recited in claim 1, wherein said preventing comprises:

storing blank content to the clipboard application instead of the designated content when said determining determines that the source file is a secured file.

8. A computer-implemented method as recited in claim 7, wherein said preventing comprises:

storing the designated content to the clipboard application when said determining determines that the source file is not a secured file.

9. A computer-implemented method as recited in claim 8, wherein said method further comprises:

receiving a paste selection to provide the designated content to the destination application;

supplying the blank content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is a secured file; and

supplying the designated content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is not a secured file.

10. A computer-implemented method as recited in claim 1, wherein said preventing comprises:

storing predetermined content to the clipboard application instead of the designated content when said determining determines that the source file is a secured file.

11. A computer-implemented method as recited in claim 10, wherein said preventing comprises:

storing the designated content to the clipboard application when said determining determines that the source file is not a secured file.

12. A computer-implemented method as recited in claim 11, wherein said method further comprises:

receiving a paste selection to provide the designated content to the destination application;

supplying the predetermined content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is a secured file; and

supplying the designated content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is not a secured file.

13. A computer-implemented method as recited in claim 1, wherein said preventing comprises:

storing scrambled content to the clipboard application instead of the designated content when said determining determines that the source file is a secured file.

14. A computer-implemented method as recited in claim 13, wherein said preventing comprises:

storing the designated content to the clipboard application when said determining determines that the source file is not a secured file.

15. A computer-implemented method as recited in claim 14, wherein said method further comprises:

receiving a paste selection to provide the designated content to the destination application;

supplying the scrambled content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is a secured file; and

supplying the designated content from the clipboard application to the destination application in response to the paste selection when said determining determines that the source file is not a secured file.

16. A computer-implemented method for restricting use of a clipboard application in a multi-application computing environment, said method comprising:

receiving a copy selection associated with designated content of a source file being displayed by a source application;

determining whether the source file is a secured file; and preventing storage of the designated content to the clipboard application when said determining determines that the source file is a secured file.

17. A computer-implemented method as recited in claim 16, wherein said method further comprises:

storing alternate content to the clipboard application in place of the designated content when said determining determines that the source file is a secured file.

18. A computer-implemented method as recited in claim 17, wherein the alternate content is one of blank content, predetermined content and scrambled content.

19. A computer-implemented method as recited in claim 17, wherein said computer-implemented method further comprises:

permitting storage of the designated content to the clipboard application when said determining determines that the source file is not a secured file.

20. A computer-implemented method as recited in claim 16, wherein said computer-implemented method further comprises:

permitting storage of the designated content to the clipboard application when said determining determines that the source file is not a secured file.

21. A computer-implemented method as recited in claim 20, wherein said determining operates to determine that the source file is a secured file based on security information provided by the source application.

22. A computer-implemented method as recited in claim 21, wherein the security information pertains to the source document.

23. A computer-implemented method for restricting use of a clipboard application in a multi-application computing environment, said method comprising:

receiving a copy selection associated with designated content of a source file being displayed by a source application;

initially storing the designated content to the clipboard application;

subsequently determining whether the source file is a secured file; and

replacing the designated content stored in the clipboard application with alternate content when said determining determines that the source file is a secured file.

24. A computer-implemented method as recited in claim 23, wherein the alternate content is one of blank content, predetermined content and scrambled content.

25. A computer-implemented method as recited in claim 24, wherein said determining operates to determine that the source file is a secured file based on security information provided by the source application.

26. A computer-implemented method for restricting use of a clipboard application in a multi-application computing environment, said method comprising:

launching a first application when a request to access a file is received;

determining, in an operating system supporting the multi-application computing environment, whether the file being requested is secured; and

loading the file in clear mode into the first application while activating a clipboard security monitor when the file is determined to be secured, wherein the clipboard security monitor ensures that no contents in the secured file can be copied into a second application.

27. A method as recited in claim 26, wherein the secured file includes a header and an encrypted portion having the contents, the header including information regarding a file key or the file key itself to be used to decrypt the encrypted portion, and

wherein said determining of whether the file is secured comprises looking for the header in the file.

28. A method as recited in claim 27, wherein the loading of the file in clear mode into the first application comprises decrypting the encrypted portion using the file key.

29. A method as recited in claim 26, wherein the clipboard security monitor is a process to control a memory space allocated to a clipboard and active in the operating system only when the file is determined secured.

30. A method as recited in claim 29, wherein said method further comprises:

receiving a portion or all of the contents of the secured file to be copied into the memory space.

31. A method as recited in claim 30, wherein the process is configured to block the portion or the all of the contents of the secured file from being copied into the memory space.

32. A method as recited in claim 30, wherein the process is configured to replace the portion or the all of the contents of the secured file with alternate contents and store the alternate contents into the memory space.

33. A method as recited in claim 30, wherein the process is configured to scramble the portion or the all of the contents of the secured file before the portion or the all of the contents are copied into the memory space.

34. A method as recited in claim 30, wherein said method further comprises:

receiving the portion or the all of the contents in the clipboard; and

determining if the second application is same as the first application when a request to paste the portion or the all of the contents in the memory space to the second application is received.

35. A method as recited in claim 34,

wherein the process is configured to prevent the portion or the all of the contents in the memory space from being copied into the second application if the second application is not same as the first application, and

wherein the process is configured to permit the portion or the all of the contents in the memory space to be copied into the second application if the second application is same as the first application.

36. A method as recited in claim 30, wherein the portion or the all of the contents of the secured file includes various objects separated by one or more spaces, and the process is configured to replace the spaces with one or more special marks before the portion or the all of the contents are copied into the memory space.

37. A method as recited in claim 36, wherein the objects are one or more of (i) words, (ii) graphs, (iii) images, (iv) tags and (v) fonts.

38. A method as recited in claim 36, wherein the special marks are ignorant to an application program.

39. A method as recited in claim 36, wherein the special marks are neither visible on a display nor printable by a printer.

40. A computer readable medium including at least computer program code for restricting use of a clipboard application in a multi-application computing environment, said computer readable medium comprising:

computer program code for receiving a copy selection associated with designated content of a source file being displayed by a source application;

computer program code for determining whether the source file is a secured file; and

computer program code for preventing subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file.